PCT/KR 00/00875
RO/KR 09.08.2000.

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 19727 호
Application Number

출 원 년 월 일 : 2000년 04월 14일
Date of Application

출 원 인 : 주식회사 시큐브
Applicant(s)

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

2000 년 07 월 11 일

특 허 청
COMMISSIONER

출력 일자: 2000/7/14

【서류명】 출원인명의변경신고서
【수신처】 특허청장
【제출일자】 2000.05.03
【구명의인】
【성명】 홍기융
【출원인코드】 420000171702
【구명의인】
【성명】 이민구
【출원인코드】 420000171719
【구명의인】
【성명】 은유진
【출원인코드】 420000171692
【구명의인】
【성명】 김재명
【출원인코드】 420000171725
【신명의인】
【성명】 주식회사 시큐브
【출원인코드】 120000214785
【사건의 표시】
【출원번호】 1020000019727
【출원일자】 2000.04.14
【발명(고안)의 명칭】 전자서명 인증기반 파일시스템 해킹방지용 보안커널 방법
【변경원인】 전부양도
【취지】 특허법 제38조제4항·실용신안법 제20조·의장법 제24조 및 상표법 제12조제1항의 규정에 의하여 위와 같이 신고합니다
.
【수수료】 13000
【첨부서류】 양도증 1통 인감증명서(양도인)4통

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 0001
【제출일자】 2000.04.14
【국제특허분류】 H04K
【발명의 명칭】 전자서명 인증기반 파일시스템 해킹방지용 보안커널 방법
【발명의 영문명칭】 Digital Signature Certificate Based Security Kernel for File System Protection

【출원인】
【성명】 은유진
【출원인코드】 4-2000-017169-2
【특기사항】 출원인대표자
【지분】 25/100

【출원인】
【성명】 홍기융
【출원인코드】 4-2000-017170-2
【지분】 25/100

【출원인】
【성명】 이민구
【출원인코드】 4-2000-017171-9
【지분】 25/100

【출원인】
【성명】 김재명
【출원인코드】 4-2000-017172-5
【지분】 25/100

【발명자】
【성명】 은유진
【출원인코드】 4-2000-017169-2

【발명자】
【성명】 홍기융
【출원인코드】 4-2000-017170-2

1020000019727 2000/7/1

【발명자】

【성명】 이민구

【출원인코드】 4-2000-017171-9

【발명자】

【성명】 김재명

【출원인코드】 4-2000-017172-5

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 출원인
은유진 (인) 출원인
홍기웅 (인) 출원인
이민구 (인) 출원인
김재명 (인)

【수수료】

【기본출원료】 20 면 39,000 원

【가산출원료】 12 면 40,800 원

【우선권주장료】 0 건 0 원

【심사청구료】 7 항 333,000 원

【합계】 412,800 원

【감면사유】 개인 (70%감면)

【감면후 수수료】 123,900 원

【첨부서류】 1. 요약서·명세서(도면)_1통 2.지분약정서_1통 3.대표자선임증_1통

【요약서】

【요약】

본 발명은 전자서명 인증에 기반한 파일시스템 해킹방지용 보안커널에 관한 것으로, 특히 세계 주요기관 및 회사의 웹서버들이 해킹(Hacking) 공격으로 인해 홈페이지 변조 및 파괴되는 사건과 같은 각종 사이버 테러 등으로 인하여 국가 기관 및 회사의 신뢰성을 실추시키는 내용으로 위·변조

커널레벨에서 원천적으로 방지할 수 있어 파일시스템에 대한 안전·신뢰성을 보장할 수 있다.

【대표도】

도 2

【색인어】

전자서명, 인증, 인증서, 커널, 보안커널, 운영체제, 접근권한, 접근제어, 웹보안, 해킹방지, 파일시스템 보호

【명세서】

【발명의 명칭】

전자서명 인증기반 파일시스템 해킹방지용 보안커널 방법{Digital Signature Certificate Based Security Kernel Method for File System Protection}

【도면의 간단한 설명】

제1도는 본 발명이 적용되는 인터넷 등 정보통신망과 서버 컴퓨터, 보안관리자, 사용자, 보안관리자 및 사용자의 컴퓨터와 이에 속한 스마트카드 및 플로피디스켓 등과 같은 저장장치를 포함하는 하드웨어 구성도

제2도는 본 발명이 적용되는 서버 컴퓨터 시스템에서의 보안관리모듈, 보안라이브러리, 인증서 저장부 등의 사용자레벨에서의 구성요소, 시스템호출 인터페이스 및 래퍼에서의 커널 등 커널레벨에서의 구성요소 및 상호동작도

제3도는 보안커널의 내부 구성 및 상호동작도

제4도는 인증서 저장부의 구성도

제5도는 보안커널 내부의 프로세스 보안정보 저장소의 구성도

제6도는 보안커널 내부의 파일시스템 보안정보 저장소의 구성도

제7도는 본 발명의 전체흐름 개략도

제8도는 본 발명의 설치단계를 기술하기 위한 실행 및 제어 흐름도

제9도는 본 발명의 운영단계를 기술하기 위한 실행 및 제어 흐름도

제10도는 운영단계 중 전자서명 인증기반 신분확인 처리 절차를 기술하기 위한 실행 및 제어 흐름도

제11도는 운영단계 중 사용자 등록 및 삭제 처리 절차를 기술하기 위한 실행 및 제어 흐름도

제12도는 운영단계 중 파일시스템 접근권한 설정 처리 절차를 기술하기 위한 실행 및 제어 흐름도

제13도는 운영단계 중 파일시스템 접근 처리 절차를 기술하기 위한 실행 및 제어 흐름도

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】 본 발명은 전자서명 인증에 기반한 해킹방지용 보안커널에 관한 것으로, 특히 홈페이지의 불법 위·변조 등 파일시스템에 대한 해킹(Hacking) 위협을 커널레벨에서 원천적으로 방지하여 서버 컴퓨터 시스템을 안전하게 하기 위한 보안커널에 관한 것이다.

<15> 이와 관련한 종래의 기술은 서버 컴퓨터를 안전하게 하기 위하여 침입차단시스템을 사용하여 특정 서비스 및 네트워크 주소에 관련된 네트워크 접속 만을 허용하는 방법 및 서버 컴퓨터 사용자에 대한 신분확인 방법을 일회용패스워드 방법 등으로 하는 등 부분적인 보안 기술 및 방법을 적용하는 제한적인 보안기능만이 제공되었다.

<16> 그러나, 특정 서비스 및 네트워크 주소에 대한 네트워크 접속만으로도 시스템 관리자 및 사용자의 권한을 획득하는 해킹 기법들이 등장함으로써 침입차단시스

템만으로는 홈페이지 등 파일시스템에 대한 위·변조를 시도하는 악의적인 해킹 행위를 원천적으로 방지 할 수 없으며, 일회용 패스워드 방법 또한 다양한 공격 방법 등이 대두되게 되어 그나마 있던 부분적인 보안기능 마저도 무력하게 되는 보안 위협이 계속적으로 발생하고 있다.

이는 응용프로그램 또는 사용자 레벨, 그리고 네트워크 레벨에서 보안기능을 제공하는 기존의 보안기술 및 방법이 컴퓨터 운영체제가 가지고 있는 근본적인 보안 취약점으로 인하여 파일시스템 위·변조를 완벽하게 방지하기가 어렵다는 문제점을 가지고 있기 때문이다.

【발명이 이루고자 하는 기술적 과제】

따라서 본 발명은 상기와 같은 문제점을 해결하기 위해 컴퓨터 운영체제의 커널 레벨에서 파일시스템 위·변조 방지를 위한 접근제어 기능을 갖는 보안커널을 추가하여 기존의 컴퓨터 운영체제내의 커널이 갖는 근본적인 보안 취약점을 해결함으로써 서버 컴퓨터 시스템을 안전·신뢰성 있게 운영할 수 있도록 하는데 그 목적이 있다.

<19> 이와 같은 목적을 달성하기 위해 본 발명은 전자서명 인증 및 검증 방법을 이용하여 사용자의 신분확인을 수행하고 신분확인된 결과를 토대로 수행되는 프로세스가 특정 파일시스템에 대한 접근 권한을 갖도록 하는 단계, 상기 단계 후 해당 프로세스 및 해당 프로세스의 자식 프로세스(child process)가 파일시스템에 접근을 시도할 경우 접근권한을 확인하는 단계로 이루어지며, 상기 단계 모두를 보안커널의 형태로 커널내부에서 동작하게 함으로써 서버 시스템의 파일에 대한 접근제어를 커널레벨에서 원천적으로 안전하게 통제하여 홈페이지등의 파일시스템 위·변조 문제를 해결하는데 그 특징이 있다.

【발명의 구성 및 작용】

<20> 이를 위해 본 발명은 사용자레벨에는 보안관리모듈, 인증서 저장부 및 보안 라이브러리를, 커널레벨에는 시스템호출 인터페이스와 보안커널로 구성한다. 보안관리모듈은 보안라이브러리와 시스템 호출 인터페이스 및 기존의 라이브러리와 상호 동작하여 보안 관리자 및 사용자용 전자서명키를 생성하고 인증서를 발급하며, 커널레벨에서 보안관리하고 적인 보안 정책과 사용자를 식별하여 파일시스템에 대한 접근제어를 완전하게 수행할 수 있도록 하는 기능을 가지고 인터페이스를 제공한다.

<21> 보안커널에서는 보안관리자 및 사용자의 신분확인을 위해 전자서명 검증의 수단을 사용자에게 공하며, 전자서명 검증 후 부여된 보안관리자 또는 사용자 프로세스의 접근권한과 보안 운영체제의 커널관리자에 의해 파일시스템 보안을 위하여 설정된 파일시스템의 접근권한 정보를 이용하여 설정 및 검사하여 특정 파일에 대한 접근제어 수단을 제공한다.

<22> 이러한 본 발명에 따른 전자서명 인증기반 파일시스템 해킹방지용 보안커널 방법을 첨부된 도면에 의거하여 상세하게 설명하면 다음과 같다.

<23> 제1도는 본 발명이 적용되는 인터넷 등 정보통신망과 서버 컴퓨터, 보안관리자, 사용자, 보안관리자 및 사용자의 컴퓨터와 이에 속한 스마트카드 및 플로피디스켓 등과 같은 저장장치를 포함하는 하드웨어 구성도로, 서버 컴퓨터(1)를 관리하는 보안관리자(5)가 플로피디스켓(3) 또는 스마트카드(4)를 가지고 전자서명 인증에 기반한 신분확인 과정을 거쳐 서버 컴퓨터(1) 및 사용자(9 또는 14)에 대한 보안관리를 책임지며, 사용자는(9)는 사용자의 플로피디스켓(7) 또는 스마트카드(8)를 가지고 전자서명 인증에 기반한 신분확인 과정을 거친 후 보안관리자에 의해 설정된 접근이 허가된 파일에 대해서만 접근 권한을 갖는다. 또한 원격 사용자(14)는 자신의 플로피디스켓(12) 또는 스마

트카드(13)를 가지고 인터넷 등 정보통신망(10)을 통해 전자서명 인증에 기반한 신분확인 과정을 거친 후 사용자에게 접근이 허가된 파일에 대해서만 접근하여 작업을 수행한다.

<24> 제2도는 본 발명이 적용되는 서버 컴퓨터(1)에서의 보안관리모듈(201), 보안라이브러리(203), 인증서 저장부(202) 등의 사용자레벨에서의 구성요소, 시스템호출 인터페이스(204) 및 보안커널(205) 등 커널레벨에서의 구성요소 및 상호동작도를 나타낸다. 사용자레벨은 보안관리모듈(201)과 인증서 저장부(202), 보안라이브러리(203)로 구성되며 보안관리모듈(201)은 보안라이브러리(203)와 시스템 호출 인터페이스(204)를 통해 보안라이브러리와 상호 동작하여 보안관리자, 사용자(9) 및 원격사용자(14)용 전자서명키를 생성하고 인증서를 발급하며, 커널레벨에서 보안관리자와 사용자를 식별하여 파일시스템에 대한 접근제어를 안전하게 수행할 수 있도록 인터페이스를 제공한다.

<25> 커널레벨은 시스템호출 인터페이스(204)와 보안커널(205)로 구성되는 것으로, 시스템호출 인터페이스(204)는 사용자레벨의 작업을 파일 서브시스템부와 프로세스 제어서브시스템부 및 보안커널(205)과의 인터페이스 역할을 수행하며, 보안커널(205)은 전자서명 검증, 접근권한 설정 및 조회, 파일시스템 접근제어 등의 기능을 수행한다.

<26> 제3도는 보안커널(205)의 내부 구성 및 상호동작도로, 접근권한 제어부(301), 전자서명검증부(302), 접근권한 설정/조회부(303), 보안정책 규칙 설정/조회부(306), 파일시스템 접근권한 결정부(307), 보안관리자 인증서 저장소(308), 프로세스 보안정보 저장소(309), 보안정책규칙 저장소(310), 파일시스템 보안정보 저장소(311)로 구성된다. 접근권한 제어부(301)는 접근권한 설정/조회부(303), 보안정책규칙 설정/조회부(306), 파일시스템 접근권한 결정부(307)의 기능 수행을 제어한다. 접근권한 설정/조회부(303)

는 프로세스 보안정보 설정/조회부(304)와 파일시스템 보안정보 설정/조회부(305)로 구성되는 것으로, 전자서명 검증부(302)를 통하여 접근을 시도하는 사용자의 신분이 확인되면 프로세스 보안정보 설정/조회부(304)를 통해 프로세스보안정보 저장소(309)의 정보를 설정하고, 파일시스템 보안정보 설정/조회부(305)는 프로세스 보안정보저장소(309)의 정보를 참조하여 파일시스템 보안정보 저장소(311)를 설정 및 조회한다. 보안정책규칙 설정/조회부(306)는 보안정책규칙 저장소(310)에 저장된 보안정책규칙을 설정 및 조회하는 기능을 수행하며, 접근권한 설정/조회부(303) 및 파일시스템 접근권한 결정부(307)와 상호연동하여 보안정책규칙에서 정한 바에 따라 접근을 허가할 것인지 여부를 결정한다. 파일시스템 접근권한결정부(307)는 프로세스보안정보 저장소(309)와 파일시스템 보안정보 저장소(311)의 정보를 보안정책규칙 설정/조회부(306)를 통하여 상호 비교하여 파일시스템 접근권한을 최종적으로 판단하는 기능을 수행한다.

<27> 제4도는 인증서 저장부(202)의 세부 구성도로, 사용자 ID(401)와 사용자 인증서(402)로 구성된다. 사용자 인증서는 사용자(9 또는 14)에게 사용자 인증서를 발행한 보안관리자(5)의 보안관리자 ID(403), 인증서의 소유자인 사용자 ID(404), 사용자의 접근권한을 나타내는 접근제어 ID(405), 사용자의 파일시스템에 대한 접근가능 유효기간을 나타내는 접근 유효기간(406), 사용자의 전자서명 공개키를 나타내는 공개키(407), 인증서의 발행시점을 나타내는 인증서 발행시간(408), 인증서의 유효한 기간을 나타내는 인증서 유효기간(409), 상기 정보(403, 404, 405, 406, 407, 408, 409)에 대하여 보안관리자가 전자서명한 결과인 전자서명값(410)으로 구성된다.

<28> 제5도는 보안커널(205) 내부의 프로세스 보안정보 저장소(309)의 세부 구성도로, 사용자(9 또는 14)가 실행한 각각의 프로세스를 식별하기 위한 프로세스 ID(501), 해당

프로세스가 보안관리자에 의하여 수행되는 프로세스임을 나타내는 보안관리자 플래그(502), 해당 프로세스에게 허용된 접근 권한을 나타내는 접근제어 ID(503)로 구성된다.

<29> 제6도는 보안커널(205) 내부의 파일시스템 보안정보 저장소(311)의 세부 구성도로, 파일을 식별할 수 있는 파일 ID(601)와 해당 파일에 접근할 수 있는 접근권한을 나타내는 접근제어 ID(602)로 구성된다.

<30> 제7도는 본 발명의 전체흐름 개략도로 다음과 같은 단계로 수행된다.

<31> 단계 1. 초기에 보안관리자(5)를 설정하는 설치단계(701)를 수행한다.

<32> 단계 2. 사용자 등록/삭제 및 파일 접근권한을 제어하는 운영단계(702)를 수행한다.

<33> 단계 3. 시스템 종료인지 판단하여(703) 종료가 아니면 단계 2로 가고 종료이면 종료한다(704).

<34> 제8도는 본 발명의 설치단계(701)를 기술하기 위한 실행 및 제어 흐름도로 다음과 같은 단계로 수행된다.

<35> 단계 1. 실행이 시작되면 보안관리자 SM(5)은 자신의 전자서명키쌍인 공개키 PK_SM과 비밀키 SK_SM을 생성한다(801).

<36> 단계 2. 보안관리자 SM(5)은 자신의 접근권한 ACID_SM 및 공개키 PK_SM을 자신의 비밀키 SK_SM으로 전자서명한 인증서 CERT_SM = SM[ACID_SM, PK_SM]SK_SM을 생성한다(802).

<37> 단계 3. 보안관리자 SM(5)는 자신의 비밀키 SK_SM을 암호화하여 스마트카드(4) 또는 플로피디스켓(3) 등에 저장한다(803).

<38> 단계 4. 보안관리자 SM(5)은 자신이 생성한 인증서 CERT_SM을 스마트카드 또는 플로피디스켓(3) 등에 저장하고(804) 이를 보안커널 SK(205) 내부의 보안관리자 인증서저장소(308)에 내장시킨다(805).

<39> 단계 5. 실행이 종료된다(806).

<40> 제9도는 본 발명의 운영단계(702)를 기술하기 위한 실행 및 제어 흐름도로 다음과 같은 단계로 수행된다.

<41> 단계 1. 서버 시스템에 접근하는 보안관리자(5) 또는 사용자(9 또는 14)에 대한 신분확인을 전자서명 인증에 기반하여 수행한다(901).

<42> 단계 2. 신분확인 결과를 판단하여(902) 신분확인 결과가 실패이면 종료하고(903) 가고, 시스템 신분확인 결과가 성공이면 보안커널 SK(205)의 보안관리자 인증서 저장소(308)에 내장된 보안관리자(5)의 인증서로부터 보안관리자(5)의 접근권한 ACID_SM을 읽어내어(910) 단계 3으로 간다.

<43> 단계 3. 단계 1(901)의 수행결과로 얻어진 결과값인 클라이언트 사용자의 접근권한 ACID_U와 보안관리자(5)의 접근권한 ACID_SM를 비교하여 서로 일치하면 단계 4(904)로 가고, 일치하지 않으면 단계 5(905)로 간다.

<44> 단계 4. 클라이언트 사용자 프로세스의 접근권한 ACID_UP에 보안관리자(5)의 접근권한 ACID_SM을 부여한다(904).

<45> 단계 4-1. 부여된 보안관리자(5) 접근권한을 가지고 사용자(9 또는 14) 등록 및 삭제처리(906)을 선택하면 단계 4-1-1로 가고, 파일시스템 접근권한 설정 처리(907)를 선택하면 단계 4-1-2로가며, 파일시스템 접근처리(908)을 선택하면 단계 4-1-3으로 간다.

<46> 단계 4-1-1. 보안관리자(5) 권한을 가지고 사용자 등록(9 또는 14) 및 삭제 처리(906)를 수행한 후 종료한다(912).

<47> 단계 4-1-2. 보안관리자(5) 권한을 가지고 파일시스템 접근권한 설정처리(907)를 수행한 후 종료한다(913).

<48> 단계 4-1-3. 보안관리자(5) 권한을 가지고 파일시스템 접근 처리(908)를 수행한 후 종료한다(914).

<49> 단계 5. 클라이언트 사용자(9 또는 14) 프로세스의 접근권한 ACID_UP에 사용자의 접근권한 ACID_U를 부여한다(905).

<50> 단계 5-1. 파일시스템 접근 처리(909)를 수행하고 종료한다(915).

<51> 제10도는 운영단계 중 전자서명 인증기반 신분확인 처리(901) 절차를 기술하기 위한 제어 흐름도로 다음과 같은 단계로 수행된다.

<52> 단계 1. 서버시스템 S가 난수 R을 생성한다(1001).

<53> 단계 2. 난수 R에 대한 전자서명값 X=U[R]SK_U를 생성한다(1002).

<54> 단계 3. 보안커널(205)내의 보안관리자 인증서 저장소(308)에 내장된 보안관리자(5)의 인증서 CERT_SM(1004)으로부터 보안관리자(5)의 공개키 PK_SM을 추출한다(1003).

<55> 단계 4. 보안커널(205)이 보안관리자(5)의 공개키 PK_SM을 이용해 클라이언트 사용자(9 또는 14)의 인증서 CERT_U를 검증하고(1005), 검증결과가 성공이면 단계 5로 가고, 검증이 실패하면, FALSE 값을 가지고 종료한다(1011).

<56> 단계 5. 클라이언트 사용자(9 또는 14)의 인증서 CERT_U로부터 클라이언트 사용자의 공개키 PK_U와 클라이언트 사용자의 접근권한 ACID_U를 추출한다(1007).

<57> 단계 6. 난수 R에 대하여 생성된 전자서명값 X를 검증하고(1008), 검증결과가 성공이면 클라이언트 사용자(9 또는 14)의 접근권한 ACID_U 값을 가지고 종료하며(1010), 검증이 실패하면, FALSE 값을 가지고 종료한다(1011).

<58> 제11도는 운영단계 중 사용자(9 또는 14) 등록 및 삭제 처리(906) 절차를 기술하기 위한 실행 및 제어 흐름도로 다음과 같은 단계로 수행된다.

<59> 단계 1. 클라이언트 사용자(9 또는 14) 프로세스의 접근권한 ACID_UP가 보안관리자(5)의 접근권한 ACID_SM과 비교하여(1101) 서로 일치하면 단계 2로 가고 일치하지 않으면 종료한다(1111).

<60> 단계 2. 보안관리자(5)의 접근권한으로 사용자(9 또는 14)의 삭제를 선택하면 단계 3으로 가고, 사용자(9 또는 14) 등록을 선택하면 단계 4로 간다(1102).

<61> 단계 3. 보안관리자(5)의 접근권한으로 등록된 사용자 U를 삭제하고(1103), 사용자 계속을 선택하면 단계 2로 가고, 종료를 선택하면 종료(1109) 한다.

<62> 단계 4. 새로운 사용자(9 또는 14) 접근권한 ACID_U를 부여한다(1104).

<63> 단계 5. 새로운 사용자(9 또는 14)의 공개키 PK_U와 비밀키 SK_U를 생성 한다(1005).

<64> 단계 6. 보안관리자 SM(5)은 새로운 사용자(9 또는 14)의 접근권한 ACID_U 및 공개키 PK_U를 보안관리자(5) 자신의 비밀키 SK_SM으로 전자서명한 인증서 CERT_U = SM[ACID_U, PK-U]SK_SM을 생성한다(1106).

<65> 단계 7. 사용자 U는 자신의 비밀키 SK_U를 암호화하여 스마트카드(8 또는 13) 또는 플로피디스켓(7 또는 12) 등에 저장한다(1107).

<66> 단계 8. 사용자 U는 자신의 인증서 CERT_U를 스마트카드(8 또는 13) 또는 플로피디스켓(7 또는 12) 등에 저장하고(1108), 사용 계속을 선택하면 단계 2로 가고, 종료를 선택하면 실행이 종료된다(1110).

<67> 제12도는 운영단계 중 파일시스템 접근권한 설정 처리(907) 절차를 기술하기 위한 실행 및 제어 흐름도로 다음과 같은 단계로 수행된다.

<68> 단계 1. 클라이언트 사용자 프로세스의 접근권한 ACID_UP가 보안관리자(5)의 접근제어 권한 ACID_SM과 비교하여(1201) 서로 일치하면 단계 2로 가고, 일치하지 않으면 종료한다(1207).

<69> 단계 2. 보안관리자(5)는 파일 접근권한 ACID_F 설정을 위한 파일 F를 선택한다(1202).

<70> 단계 3. 보안관리자(5)는 해당파일 F에 접근을 허가할 대상 사용자를 선택한다(1203).

<71> 단계 4. 보안커널 SK는 파일 접근권한 ACID_F에 선택된 사용자의 접근권한 ACID_U를 설정한다(1204)

<72> 단계 5. 사용 계속을 선택하면 단계 2로 가고, 종료를 선택하면 실행이 종료된다(1206).

<73> 제13도는 운영단계 중 파일시스템 접근처리(908 및 909) 절차를 기술하기 위한 실행 및 제어 흐름도로 다음과 같은 단계로 수행된다.

<74> 단계 1. 보안커널(205)은 접근대상 파일 F의 이름을 얻어낸다(1301).

<75> 단계 2. 파일 F에 대해서 접근을 시도하는 클라이언트 사용자 프로세스의 접근권한

ACID_UP가 보안관리자의 접근권한 ACID_SM과 같은지 비교하여(1302) 서로 일치하면 단계3으로 가고, 일치하지 않으면 단계 4로 간다.

<76> 단계 3. 클라이언트 사용자 프로세스의 파일 F에 대한 접근을 허가하고(1303), 사용 계속을 선택하면 단계 1로 가며, 종료를 선택하면 실행이 종료된다(1307).

<77> 단계 4. 파일 F에 대해서 접근을 시도하는 클라이언트 사용자 프로세스의 접근권한이 보안관리자의 ACID_UP가 사용자의 접근권한 ACID_U와 같은지 비교하여(1304), 관리자의 접근권한을 가지고 있으면 단계 5로 가고, 그렇지 않으면 종료(1308)한다.

<78> 단계 5. 파일 F에 대해서 접근을 시도하는 클라이언트 사용자 프로세스의 접근권한이 ACID_UP가 파일 접근권한 ACID_F와 같은지 비교하여(1305), 같으면 단계 6으로 가고, 같지 않으면 종료(1309)한다.

<79> 단계 6. 클라이언트 사용자 프로세스의 파일 F에 대한 접근을 허가하고(1306), 사용 계속을 선택하면 단계 1로 가며, 종료를 선택하면 실행이 종료된다(1310).

【발명의 효과】

<80> 본 발명은 시스템 설치시 커널내부의 보안커널에 보안관리자의 인증서를 내장함으로써 인증서에 대한 위·변조 등 해킹을 방지할 수 있고, 전자서명 인증기반의 신분확인 및 전자서명 검증, 프로세스 접근권한 설정, 파일시스템 접근권한 설정 및 사용자 프로세스의 파일시스템 접근제어를 모두 커널내부에서 수행하므로 서버 시스템의 파일에 대한 위·변조 등의 해킹 행위를 커널레벨에서 원천적으로 방지할 수 있어 파일시스템에 대한 안전·신뢰성을 보장할 수 있다.

<81> 특히, 홈페이지를 운영하는 웹 서버시스템에 본 발명을 적용하면 홈 페이지 위·변

조 등의 해킹 사고를 원천적으로 방지하여 안전·신뢰성 있는 홈페이지 운영을 보장받을 수 있다.

1307

로세스의 청구권한

자의 [illegible]하을

로세스의 청구권한

계 [illegible]으로 가고, 갑

[illegible]

【특허청구범위】

【청구항 1】

사용자 인증 과정을 거쳐 허가된 사용자에게 인가된 해당 파일시스템의 접근을 허용하는 컴퓨터시스템에 있어서,

서버 컴퓨터(1)에 운영체제를 설치하는 단계에서 보안관리자(5)가 전자서명키 및 이 인증서를 생성하고 이를 스마트카드(3) 및 플로피디스켓(4) 등의 저장소에 저장·관리하고 서버 컴퓨터(1)의 보안커널(205)내에 보안관리자(5)의 인증서를 보안관리자 인증서 저장소(308)에 내장시키는 1단계, 시스템 운영시 보안관리자(5)가 사용자(9) 및 원격사용자(14)를 설정하고 사용자(9) 및 원격사용자(14)를 위한 전자서명키를 각각 생성하여 보안관리자(5)의 전자서명키로 전자서명한 인증서를 각각 생성하고 사용자(9)의 스마트카드(7) 및 플로피디스켓(8), 원격사용자(14)의 스마트카드(13) 및 플로피디스켓(12) 등의 저장소에 저장·관리하는 2단계, 보안관리자(5)가 보안관리자(5)자신을 포함하여 사용자(9) 및 원격사용자(14)에게 접근을 허가하고자 하는 대상 파일시스템의 접근권한을 설정하는 3단계, 서버 컴퓨터(1)이 보안관리자(5), 사용자(9) 또는 원격사용자(14)가 접근을 시도할시 전자서명 인증에 기반하여 그 신분을 확인하고 파일시스템에 대한 접근제어를 수행하는 제4단계를 포함하는 것을 특징으로 하는 전자서명 인증기반의 파일시스템 해킹방지용 보안커널 방법,

【청구항 2】

제1항에 있어서, 보안관리자(5) 및 사용자(9 또는 14)의 인증서를 저장하는 인증서 저장부(202), 응용프로그램이나 보안관리모듈(201)이 보안커널(205)내에 정의된 보안 기

능을 이용하도록 하는 보안라이브러리(203), 보안관리모듈(201)이 보안커널(205)내의 보안기능을 호출할 수 있도록 연계시켜주는 시스템 호출 인터페이스(204), 보안관리자(5) 및 사용자(9 또는 14)에 대한 전자서명키 및 인증서를 생성하고 생성된 인증서를 인증서 저장부(202)에 저장하며 보안관리자(5) 및 사용자(9 또는 14)가 접근을 시도할시 접근권한을 허용하기 위하여 보안라이브러리(203)와 시스템호출 인터페이스(204)를 통하여 전자서명을 검증할 수 있도록 하는 상호 동작관계를 체공하는 보안관리모듈(201), 시스템 관리자(5) 및 사용자(9 또는 14)의 시스템 호출 인터페이스(204)를 통해 입력된 보안관리자(5) 및 사용자(9 또는 14)의 전자서명 검증, 파일시스템 접근권한 설정 및 조회, 보안정책규칙 설정 및 조회, 파일시스템 접근권한 결정 등의 기능을 수행하는 보안커널(205)을 특징으로 하는 전자서명 인증기반 파일시스템 해킹방지용 보안커널 방법,

【청구항 3】

제2항에 있어서, 보안커널(205)로부터 실행 요구를 입력 받아 해당 각 실행부로 작업권한을 할당하는 접근권한 제어부(301), 보안관리자의 신분을 도용하여 해킹을 시도하는 각종의 위협을 방지하기 위한 것으로 시스템 설치시 보안관리자의 인증서를 내장하는 보안관리자 인증서 저장소(308), 프로세스의 보안정보를 저장하는 프로세스 보안정보저장소(309), 파일시스템의 보안정보를 저장하는 파일시스템 보안정보 저장소(311), 프로세스와 파일시스템간의 접근제어 결정에 적용되는 보안정책규칙이 저장되는 저장소(310), 보안관리자 인증서 저장소(308)로부터 보안관리자

의 인증서를 읽어서 전자서명 검증을 수행하는 전자서명 검증부(302), 프로세스의 보안 정보를 설정관리 및 조회하는 프로세스 보안정보 설정/조회부(304)와 파일시스템의 보안 정보를 설정관리 및 조회하는 파일시스템 보안정보 설정/조회부(305)로 구성되는 접근 권한 설정/조회부(303), 프로세스 및 파일시스템의 접근제어 보안정책을 관리하고 보안 정책규칙 저장소(310)에 설정된 보안정책 규칙을 이용하여 접근권한 설정/조회부(303)의 파일시스템 접근권한 결정부(307)에 반영될 수 있도록 하는 보안정책규칙 설정/조회부(306), 사용자 프로세스의 접근권한과 파일시스템에 설정된 접근권한을 비교하여 최종적으로 파일시스템 접근제어를 수행하는 파일시스템 접근권한 결정부(307)를 특징으로 하는 전자서명 인증기반의 파일시스템 해킹방지용 보안커널 방법,

【청구항 4】

제2항의 인증서 저장부(202)에 있어서, 각 사용자에 대해 사용자 식별자인 사용자 ID(401)와 사용자 인증서(402)로 구성하고, 사용자 인증서(402)를 사용자 인증서를 발행한 보안관리자(5)의 보안관리자 ID(403), 인증서의 소유자인 사용자 ID(404), 사용자의 접근 권한을 나타내는 접근제어 ID(405), 사용자의 파일시스템에 대한 접근가능 유효기간을 나타내는 접근 유효기간(406), 사용자의 전자서명 공개키를 나타내는 공개키(407), 인증서의 발행시점을 나타내는 인증서 발행시간(408), 인증서의 유효한 기간을 나타내는 인증서 유효기간(409), 상기 정보(403, 404, 405, 406, 407, 408, 409)에 대하여 보안관리자(5)가 전자서명한 결과인 전자서명값(410)으로 구성하는 것을 특징으로 하는 전자서명 인증기반의 파일시스템 해킹방지용 보안커널 방법,

【청구항 5】

제3항의 프로세스 보안정보 저장소(309)에 있어서, 사용자가 실행한 각각의 프로세스를 식별하기 위한 프로세스 ID(501)와 해당 프로세스가 보안관리자(5)에 의하여 수행되는 프로세스임을 나타내는 보안관리자 플래그(502) 및 해당 프로세스에게 허용된 접근권한을 나타내는 접근메어 ID(503)로 구성하는 것을 특징으로 하는 전자서명 인증기반의 파일시스템 해킹방지용 보안커널 방법,

【청구항 6】

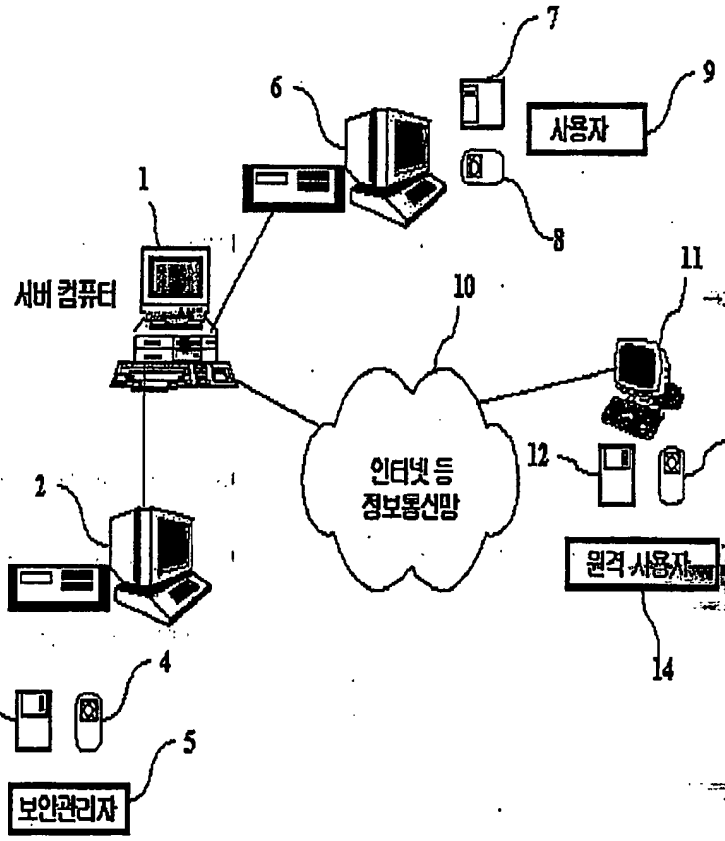
제3항의 파일시스템 보안정보 저장소(311)에 있어서, 파일을 식별할 수 있는 파일 ID(601)와 해당 파일에 접근할 수 있는 접근권한을 나타내는 접근제어 ID(602)로 구성하는 것을 특징으로 하는 전자서명 인증기반의 파일시스템 해킹방지용 보안커널 방법.

【청구항 7】

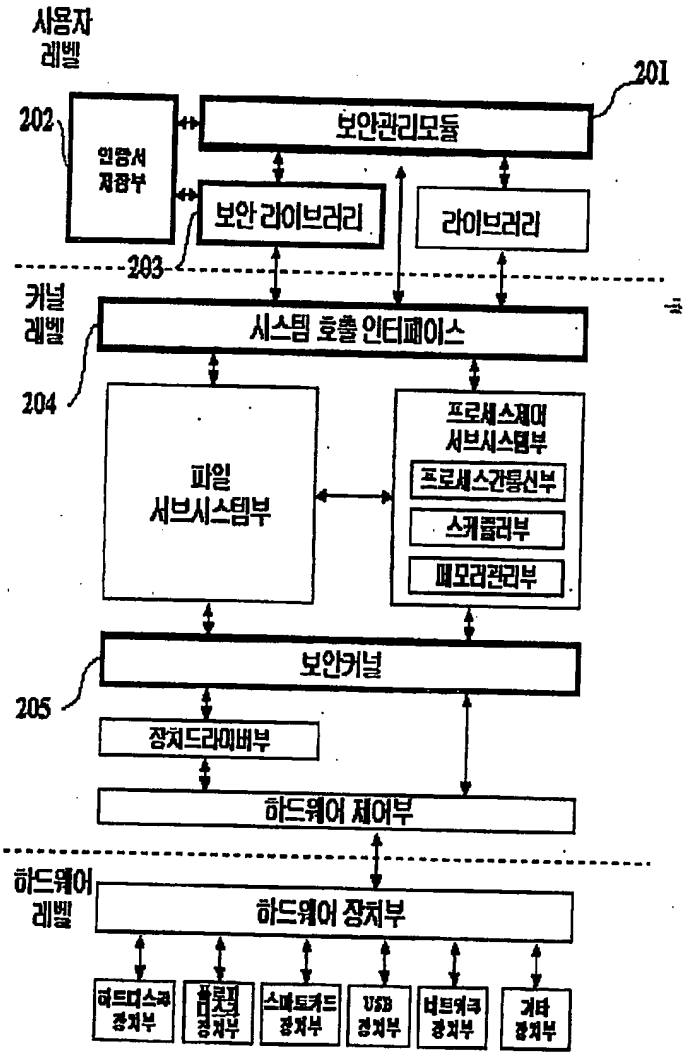
상기 제1항, 제2항, 제3항, 제4항, 제5항, 제6항이 실현되기 위한 제어 및 실행 흐름도(제8도, 제9도, 제10도, 제11도, 제12도, 제13도).

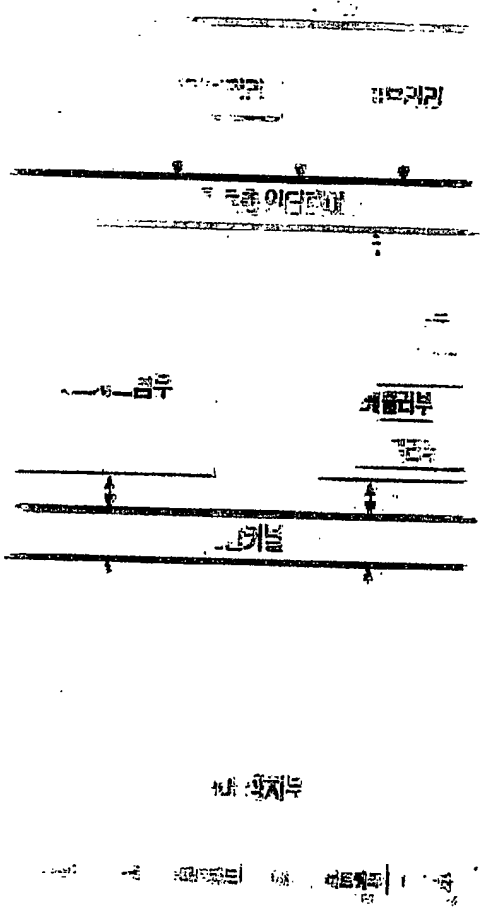
【도면】

【도 1】

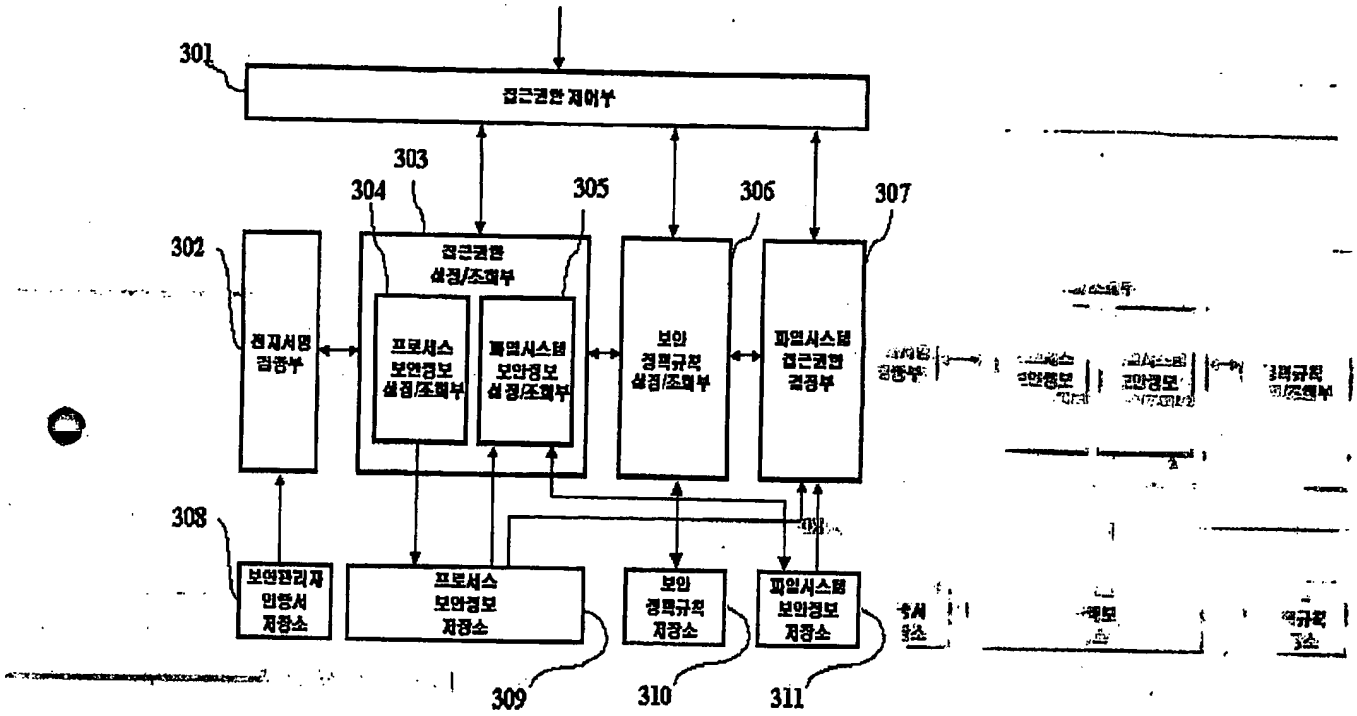


【도 2】

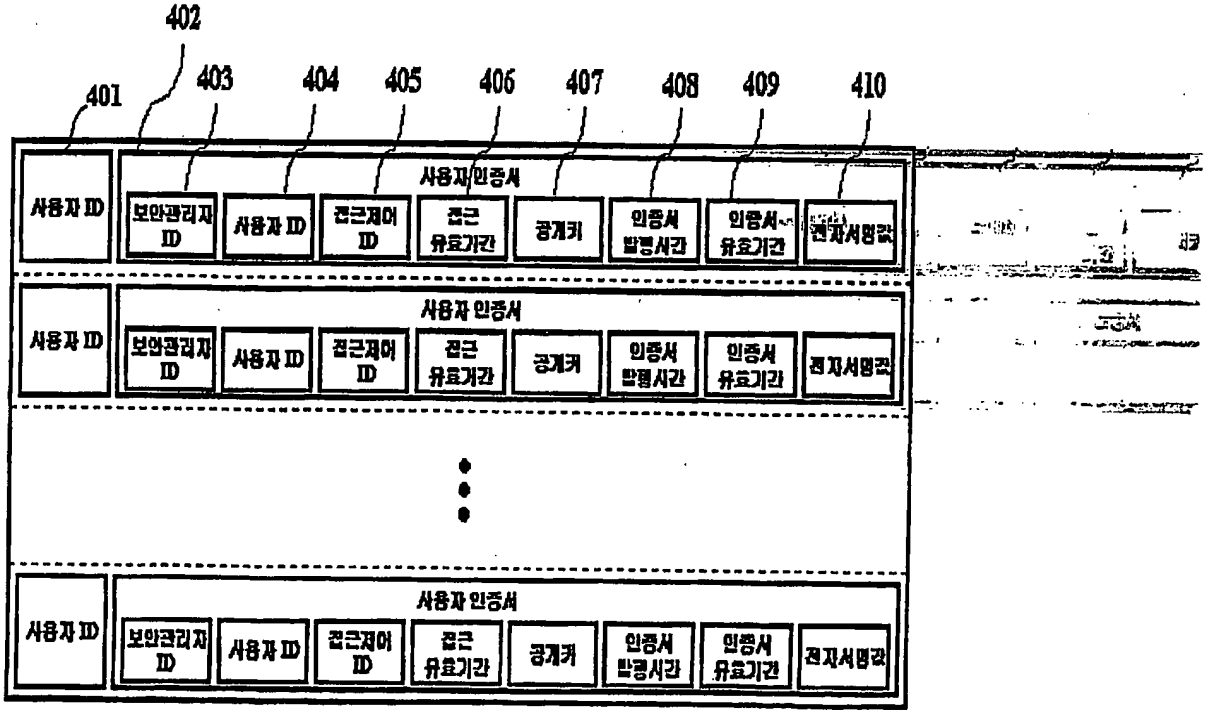

사용자
레벨
201
202
인증서
저장부
보안관리모듈
보안 라이브러리
라이브러리
203
커널
레벨
시스템 호출 인터페이스
204
파일
서브시스템부
프로세스제어
서브시스템부
프로세스간통신부
스케줄러부
메모리관리부
보안커널
205
장치드라이버부
하드웨어 제어부
하드웨어
레벨
하드웨어 장치부
하드디스크
장치부
플로피
장치부
스마트카드
장치부
USB
장치부
네트워크
장치부
기타
장치부



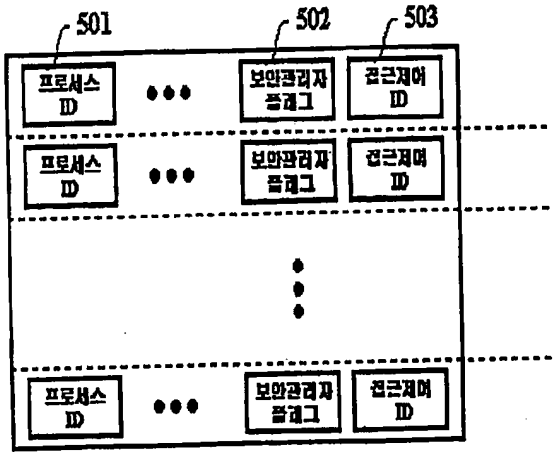
【도 3】


301
접근권한 제어부
303
304
305
306
307
302
전자서명 검증부
접근권한 설정/조회부
프로세스 보안정보 설정/조회부
파일시스템 보안정보 설정/조회부
보안 정책규칙 설정/조회부
파일시스템 접근권한 검증부
308
보안관리자 인증서 저장소
프로세스 보안정보 저장소
보안 정책규칙 저장소
파일시스템 보안정보 저장소
309
310
311

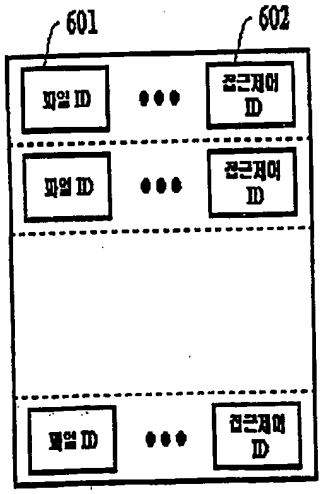
【도 4】


402
401
403
404
405
406
407
408
409
410
사용자 ID
사용자 인증서
보안관리자 ID
사용자 ID
접근제어 ID
접근 유효기간
공개키
인증서 발행시간
인증서 유효기간
전자서명값

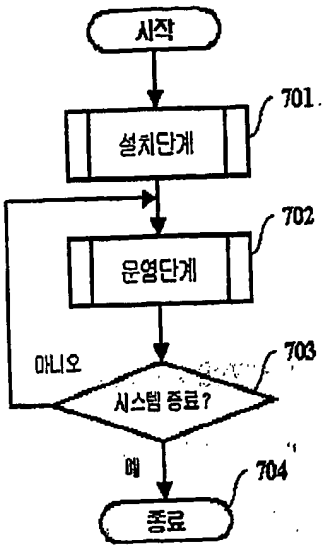
【도 5】



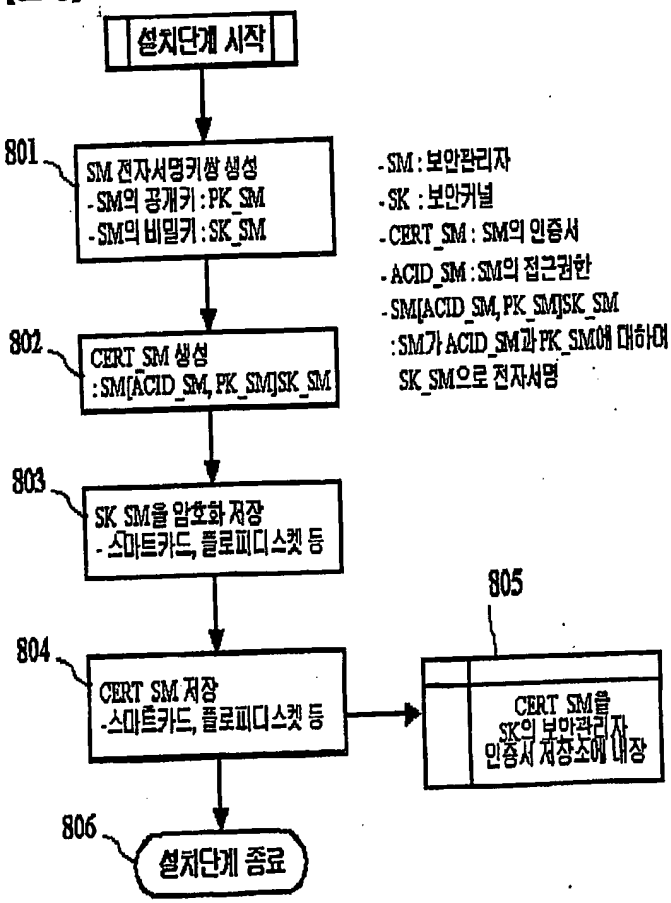
【도 6】



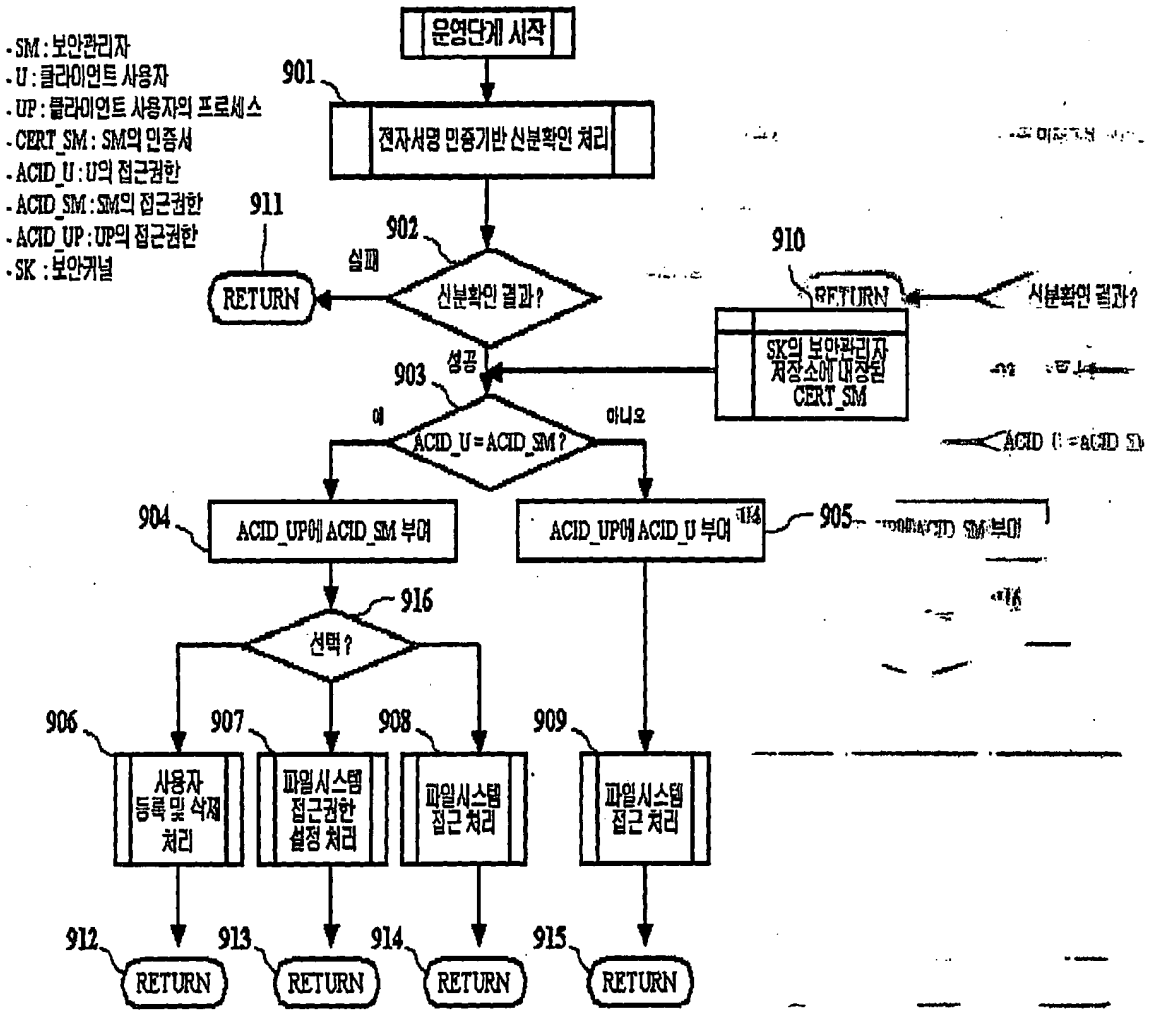
【도 7】


시작
701
설치단계
702
운영단계
아니오
703
시스템 종료?
예
704
종료

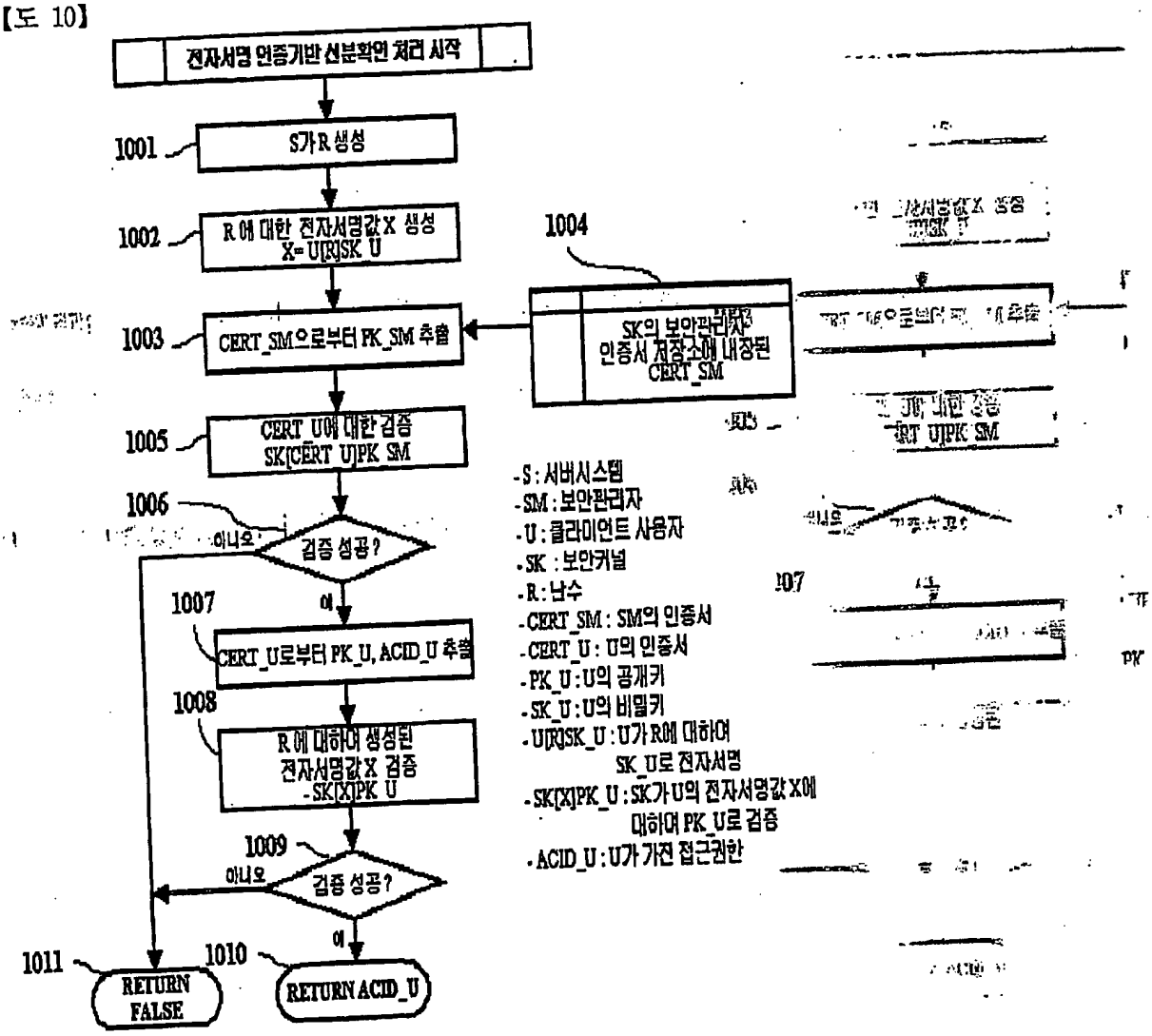
【도 8】


설치단계 시작
801
SM 전자서명키쌍 생성
-SM의 공개키 : PK_SM
-SM의 비밀키 : SK_SM
802
CERT_SM 생성
:SM[ACID_SM, PK_SM]SK_SM
803
SK_SM을 암호화 저장
- 스마트카드, 플로피디스켓 등
804
CERT SM 저장
-스마트카드, 플로피디스켓 등
805
CERT SM을
SK의 보안관리자
인증서 저장소에 내장
806
설치단계 종료
-SM : 보안관리자
-SK : 보안커널
-CERT_SM : SM의 인증서
-ACID_SM : SM의 접근권한
-SM[ACID_SM, PK_SM]SK_SM
:SM가 ACID_SM과 PK_SM에 대하여
SK_SM으로 전자서명

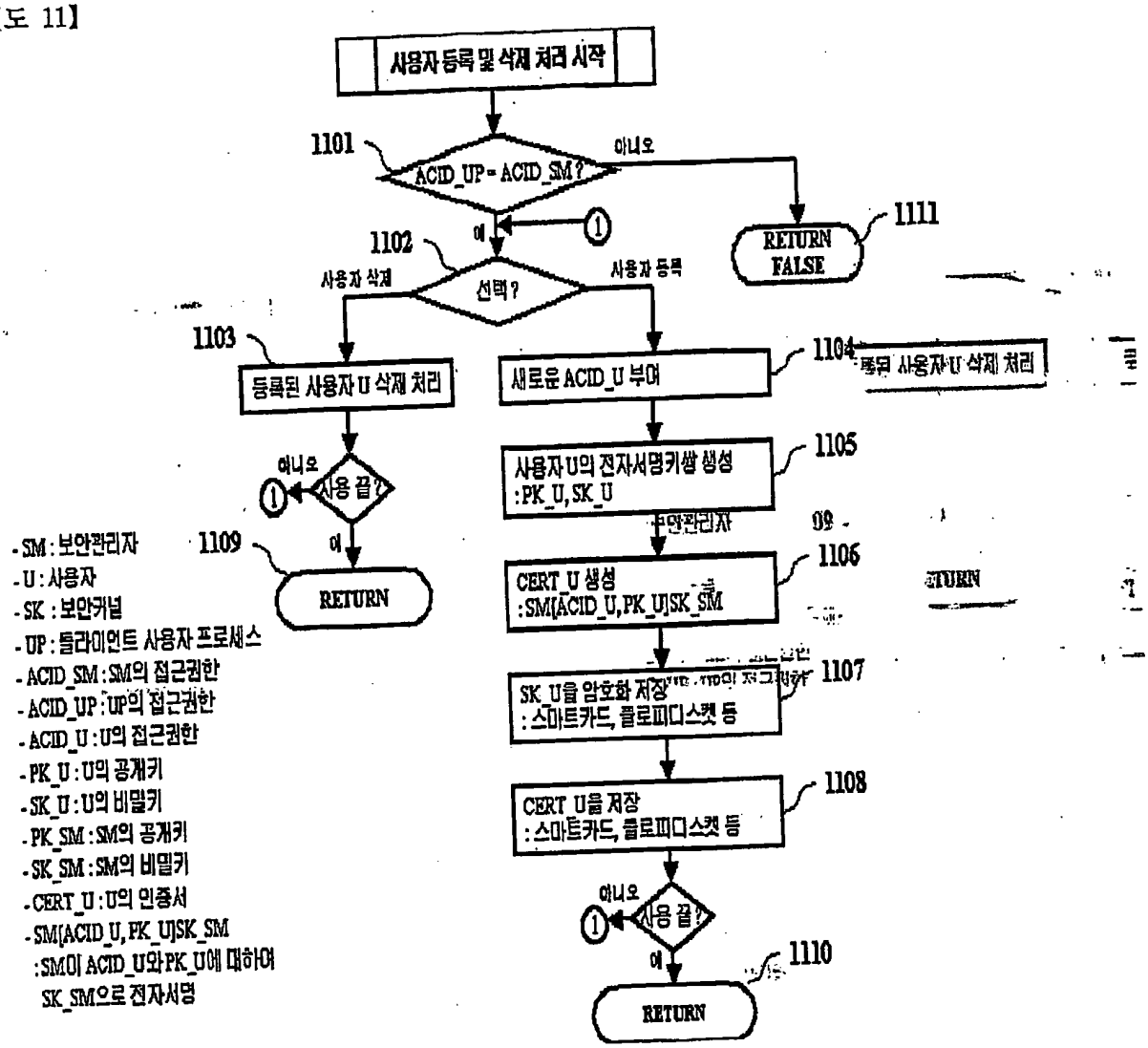
【도 9】


- SM : 보안관리자
- U : 클라이언트 사용자
- UP : 클라이언트 사용자의 프로세스
- CERT_SM : SM의 인증서
- ACID_U : U의 접근권한
- ACID_SM : SM의 접근권한
- ACID_UP : UP의 접근권한
- SK : 보안커널
운영단계 시작
901
전자서명 인증기반 신분확인 처리
902
신분확인 결과?
실패
911
RETURN
910
RETURN
신분확인 결과?
SK의 보안관리자 저장소에 대장된 CERT_SM
성공
903
ACID_U = ACID_SM?
예
아니오
904
ACID_UP에 ACID_SM 부여
ACID_UP에 ACID_U 부여
905
916
선택?
906
907
908
909
사용자 등록 및 삭제 처리
파일시스템 접근권한 설정 처리
파일시스템 접근 처리
파일시스템 접근 처리
912
913
914
915
RETURN
RETURN
RETURN
RETURN

【도 10】

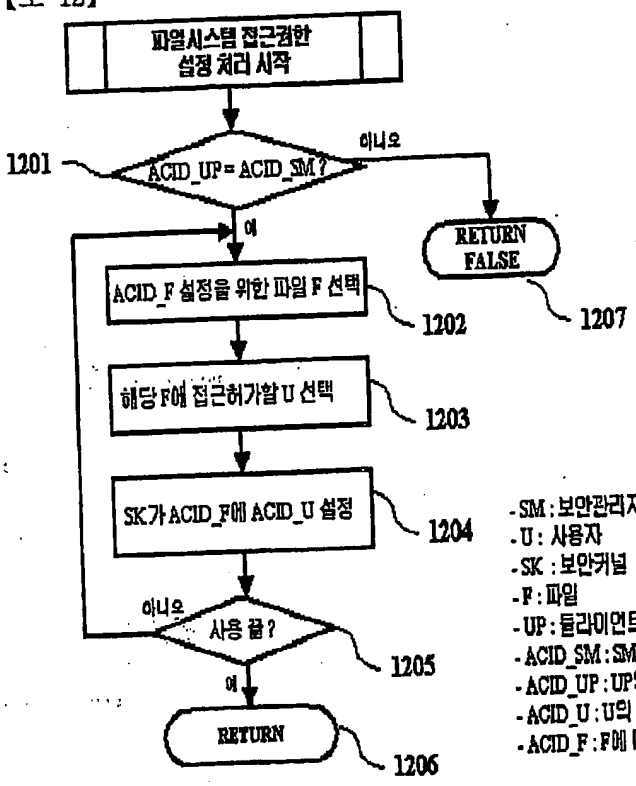

전자서명 인증기반 신분확인 처리 시작
1001
S가 R 생성
1002
R에 대한 전자서명값 X 생성
X=U[R]SK_U
1003
CERT_SM으로부터 PK_SM 추출
1004
SK의 보안관리자
인증서 저장소에 내장된
CERT_SM
1005
CERT_U에 대한 검증
SK[CERT_U]PK_SM
1006
검증 성공?
아니오
예
1007
CERT_U로부터 PK_U, ACID_U 추출
1008
R에 대하여 생성된
전자서명값 X 검증
-SK[X]PK_U
1009
검증 성공?
아니오
예
1010
RETURN ACID_U
1011
RETURN FALSE
-S : 서버시스템
-SM : 보안관리자
-U : 클라이언트 사용자
-SK : 보안커널
-R : 난수
-CERT_SM : SM의 인증서
-CERT_U : U의 인증서
-PK_U : U의 공개키
-SK_U : U의 비밀키
-U[R]SK_U : U가 R에 대하여
SK_U로 전자서명
-SK[X]PK_U : SK가 U의 전자서명값 X에
대하여 PK_U로 검증
-ACID_U : U가 가진 접근권한

【도 11】



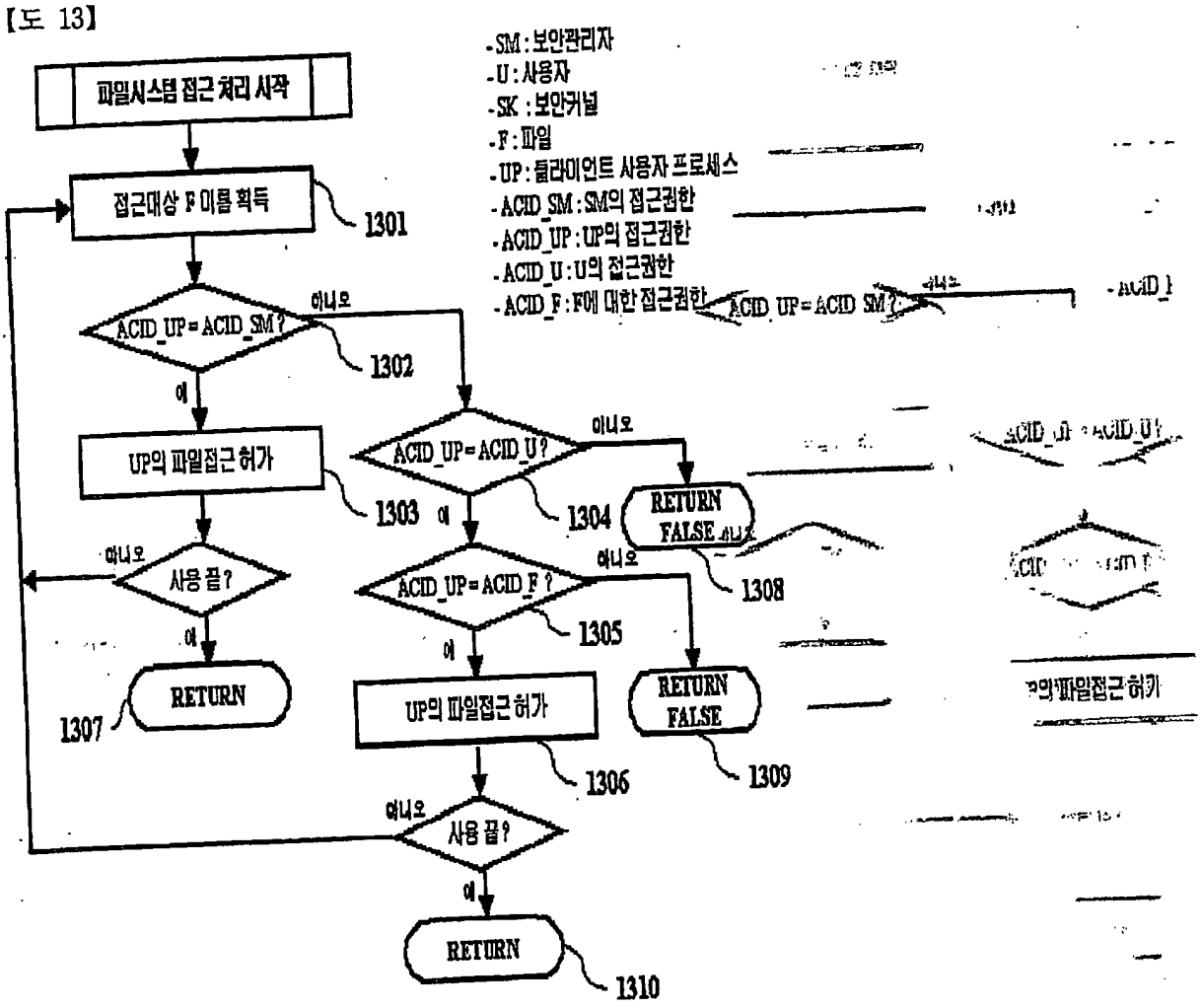
- SM : 보안관리자
- U : 사용자
- SK : 보안커널
- UP : 클라이언트 사용자 프로세스
- ACID_SM : SM의 접근권한
- ACID_UP : UP의 접근권한
- ACID_U : U의 접근권한
- PK_U : U의 공개키
- SK_U : U의 비밀키
- PK_SM : SM의 공개키
- SK_SM : SM의 비밀키
- CERT_U : U의 인증서
- SM[ACID_U, PK_U]SK_SM
  : SM이 ACID_U와 PK_U에 대하여 SK_SM으로 전자서명

【도 12】



- SM : 보안관리자
- U : 사용자
- SK : 보안커널
- F : 파일
- UP : 클라이언트 사용자 프로세스
- ACID_SM : SM의 접근권한
- ACID_UP : UP의 접근권한
- ACID_U : U의 접근권한
- ACID_F : F에 대한 접근권한

【도 13】


-SM : 보안관리자
-U : 사용자
-SK : 보안커널
-F : 파일
-UP : 클라이언트 사용자 프로세스
-ACID_SM : SM의 접근권한
-ACID_UP : UP의 접근권한
-ACID_U : U의 접근권한
-ACID_F : F에 대한 접근권한
파일시스템 접근 처리 시작
접근대상 F 이름 획득
1301
ACID_UP = ACID_SM ?
1302
아니오
예
UP의 파일접근 허가
1303
ACID_UP = ACID_U ?
1304
아니오
예
RETURN FALSE
1308
사용 끝?
아니오
예
RETURN
1307
ACID_UP = ACID_F ?
1305
아니오
예
UP의 파일접근 허가
1306
RETURN FALSE
1309
사용 끝?
아니오
예
RETURN
1310